UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/552,115	04/19/2000	Aviad Kipnis	NDS-4600 USA	3130

7590 03/24/2004

Limbach & Limbach LLP
Attn: Joel G Ackerman
2001 Ferry Building
San Francisco, CA 94111

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

RECEIVED
APR 2 0 2004
Technology Center 2100

UNITED STATES PATENT AND TR[illegible]EMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/552,115	04/19/2000	Aviad Kipnis	NDS-4600 USA	3130

7590 02/12/2004

Limbach & Limbach LLP
Attn: Joel G Ackerman
2001 Ferry Building
San Francisco, CA 94111

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	10

DATE MAILED: 02/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

RECEIVED
MAR 01 2004
Technology Center 2100

RECEIVED
MAR 03 2004
TC 2100

PTO-90C (Rev. 10/03)

Organization TC2100 Bldg./Room PK2
U. S. DEPARTMENT OF COMMERCE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
IF UNDELIVERABLE RETURN IN TEN DAYS

OFFICIAL BUSINESS

AN EQUAL OPPORTUNITY EMPLOYER

RETURN TO SENDER
Rt. #
Carr. Init.
Date

- ☒ Forwarding Order Expired Unable To Forward
- ☐ Insufficient Address
- ☐ Moved, Left No Address
- ☐ Unclaimed ☐ Refused
- ☐ Attempted - Not Known
- ☐ No Such Street ☐ Number
- ☐ Vacant ☐ Illegible
- ☐ No Mail Receptacle
- ☐ Box Closed - No Order
- ☐ ...ddress

RETURN TO SENDER
Rt. #
Carr. Init.
Date

- ☒ Forwarding Order Expired Unable To Forward
- ☐ Insufficient Address
- ☐ Moved, Left No Address
- ☐ Unclaimed ☐ Refused
- ☐ Attempted - Not Known
- ☐ No Such Street ☐ Number
- ☐ Vacant ☐ Illegible
- ☐ No Mail Receptacle
- ☐ Box Closed - No Order
- ☐ Returned For Better Address
- ☐ Postage Due

Office Action Summary	Application No.	Applicant(s)	
	09/552,115	KIPNIS ET AL.	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _16 July 2001_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-42_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _19 April 2000_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _5_.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-42 have been rejected.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-4, 11, 14, 18-21, 28, 31, and 35-36 are rejected under 35 U.S.C. 103(a) as being obvious over Patarin U.S. Pat. No. 6111952 (hereinafter Patarin) in view of Shamir U.S. Pat. No. 5375170 (hereinafter Shamir).

The applied reference has a common inventor with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art only under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 103(a) might be overcome by: (1) a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not an invention "by another"; (2) a showing of a date of invention for the claimed subject matter of the application which corresponds to subject matter disclosed but not claimed in the reference, prior to the effective U.S. filing date of the reference under 37 CFR 1.131; or (3) an oath or declaration under 37 CFR 1.130 stating that the application and reference are currently owned by the same party and that the inventor named in the application is the prior inventor under 35 U.S.C. 104, together with a terminal disclaimer in

accordance with 37 CFR 1.321(c). For applications filed on or after November 29, 1999, this rejection might also be overcome by showing that the subject matter of the reference and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person. See MPEP § 706.02(l)(1) and § 706.02(l)(2). The prior art by the inventors show limitations disclosed in this application.

As per claim 1, 18, 35 and 36, Patarin discloses a digital signature cryptographic method comprising: supplying a set S1 of k polynomial functions as a public-key (Patarin: column 3 lines 47-48), the set S1 including the functions $P_1(x_1,\ldots,x_{n+v}, y_1, \ldots, y_k),\ldots, P_k(x_1,\ldots,x_{n+v}, y_1,\ldots,y_k)$, where k, v, and n are integers, $x_1,\ldots,x_{n+v}$ are n+v variables of a first type, $y_1,\ldots,y_k$ are k variables of a second type, and the set S1 is obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_{n+v},\ldots,a_{n+v}, y_1, \ldots, y_k),\ldots, P'_k(a_1,\ldots,a_{n+v}, y_1,\ldots,y_k)$ where $a_1,\ldots, a_{n+v}$ are n+v variables which include a set of n "oil" variables $A1,\ldots,An$, and a set of v "vinegar" variables $a_{n+1},\ldots,a_{n+v}$ (Patarin: column 2 line 27 – column 3 line 21) ; applying a hash function on the message to produce a series of k values $b_1,\ldots,b_k$; substituting the series of k values $b_1,\ldots,b_k$ for the variables $y_1,\ldots y_k$ of the set S2 respectively to produce a set S3 of k polynomial functions $P''_1(a_1,\ldots,a_{n+v}),\ldots, P''(a_1,\ldots,a_{n+v})$; selecting v values $a'_{n+1},\ldots a'_{n+v}$ for the v "vinegar" variables $a_{n+1},\ldots a_{n+v}$ (Patarin: column 3 lines 49-54) ; solving a set of equations $P''_1(a_1,\ldots,a_n, a'_{n+1},\ldots,a'_{n+v}) =0,\ldots, P''_k(a_1,\ldots,a_n, a'_{n+1},\ldots,a'_{n+v}) =0$ to obtain a solution for $a'_1,\ldots,a'_n$ (Patarin: column 3 line 44-60). Patarin does not explicitly teach the method of providing a message to be signed and applying a hash function on the message to produce a series of k values $b_1,\ldots, b_k$ and applying the secret key operation to transform $a'_1,\ldots,a'_{n+v}$ to a digital signature $e_1,\ldots,e_{n+v}$. However,

Shamir discloses that limitation (Shamir: column 3 line 63 – column 4 line 5: provide the message and apply hash function; column 4 line 1-5: use the knowledge of the secret function to compute a signature). It would have been obvious to one having ordinary skill in the art to combine the teachings of Shamir within the system of Patarin because it is well known in the art to use hash function to mixed and encrypt the data and transform it into digital signature.

As per claim 2 and 19, the combination of Patarin-Shamir discloses a method according to claim 1. Patarin further discloses the method comprising the step of verifying the digital signature (Patarin: column 4 lines 1-6).

As per claim 3, 14, 20, and 31, the combination of Patarin-Shamir discloses a method according to claim 1. Patarin further discloses a method according to claim 2 and wherein said verifying step comprises: verifying that the equations $P_1(e_1,\ldots,e_{n+v}, b_1, \ldots, b_k)=0,\ldots,$ $P_k(e_1,\ldots,e_{n+v}, b_1, \ldots, b_k)=0$ are satisfied (Patarin: column 3 line 62 – column 4 line 6). Patarin does not explicitly disclose the method comprises obtaining the signature $e_1,\ldots,e_{n+v}$, the message, the hash function and the public key; applying the hash function on the message to produce the series of k values $b_1,\ldots,b_k$. However, Shamir further discloses these limitations (Shamir: column 4 lines 6-15: vi constitutes as the bi while h is the hash function and fi is the public key). It would have been obvious to one having ordinary skill in the art to combine the teachings of Shamir within the system of Patarin because it is required by the verifier to obtain certain parameters before being able to verify the signature.

As per claim 4 and 21, the combination of Patarin-Shamir discloses a method according to claim 1. Patarin further discloses the set S2 comprises the set f(a) of k polynomial functions of the HFEV scheme (Patarin: column 3 lines 16-22).

As per claim 11 and 28, the combination of Patarin-Shamir discloses a method according to claim 1. Patarin further discloses said secret key operation comprises a secret affine transformation s on the n+v variables $a_1,\ldots,a_{n+v}$ (Patarin: column 3 lines 8-25).

4. Claims 5-6, 8, 15, 22, 23, 25, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin in view of Shamir as applied to claim 1 above, and further in view of Shamir et al 'Cryptanalysis of the Oil and Vinegar Signature Scheme' (hereinafter Shamir2).

As per claim 5 and 22, the combination of Patarin-Shamir discloses a method according to claim 1. Patarin-Shamir does not explicitly disclose the set S2 comprises the set S of k polynomial functions of the UOV scheme. However, Shamir2 discloses that limitation (Shamir2: page259). It would have been obvious to one having ordinary skill in the art to combine the teachings of Patarin, Shamir, and Shamir2 because polynomial functions of different scheme can be interchangeably used to improve the security of the signature.

As per claim 6, 15, 23, and 32, the combination of Patarin-Shamir discloses a method according to claim 1. Patarin-Shamir does not explicitly disclose said supplying step comprises the step of selecting the number v of "vinegar" variables to be greater than the number n of "oil" variables. However, Shamir2 discloses that limitation (Shamir2: page 266: need to modify definition of oil and vinegar domains). It would have been obvious to one having ordinary skill in the art to combine the teachings of Patarin, Shamir, and Shamir2 because different number of variables makes it not as clearly distinguishable from the quadratic terms in the published forms thus makes it harder to attack.

As per claim 8 and 25, the combination of Patarin-Shamir discloses a method according to claim 1. Patarin further discloses said supplying step comprises the step of obtaining the set S1 from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized by that all coefficient of components involving any of the $y_1,\ldots,y_k$ variables in the k polynomial functions $P'_1(a_{n+v},\ldots,a_{n+v}, y_1, \ldots, y_k),\ldots, P'_k(a_1,\ldots,a_{n+v}, y_1,\ldots,y_k)$ are zero (Patarin: column 3 lines 5-54). Patarin-Shamir does not explicitly disclose the number v of "vinegar" variables is greater than the number of "oil" variables. However, Shamir2 discloses that limitation (Shamir2: page 266). Same rationale applies here as above in rejecting claim 6.

5. Claims 7, 9, 10, 16-17, 24, 26-27, and 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin in view of Shamir as applied to claim 1 above, and further in view of Patarin U.S. Pat. No. 5790675 (hereinafter Patarin2).

As per claim 7 and 24, the combination of Patarin-Shamir discloses a method according to claim 1. Patarin further discloses v is selected such that q^v, where q is the number of elements of a finite field K (Patarin: column 3 lines 5-22: q is the number of element of K while n is the number of variables which is equal to message or n=m). Patarin-Shamir does not explicitly disclose q^v is greater than 2^{32}. However, Patarin2 discloses that limitation (Patarin2: column 7 lines 45-50: 32 bits is equal to 2^{32}). It would have been obvious to one having ordinary skill in the art to combine the teachings of Patarin, Shamir, and Patarin2 because it ensures maximum security and prevent exhaustive search attack.

As per claim 9, 10, 16, 17, 26, 27, 33, and 34, the combination of Patarin-Shamir discloses a method according to claim 8. Patarin further discloses the set S2 comprises the set S

of k polynomial functions of the UOV scheme, and the number v of "vinegar" variables is selected so as to satisfy one of the following conditions (Patarin: column 3 lines 5-22: q is the number of element of K while n is the number of variables which is equal to message or n=m). Patarin does not explicitly disclose the conditions. However, Patarin2 discloses the limitation (a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$ (Patarin2: column 7 lines 45-50: 32 bits and preferably at 64 bits). It would have been obvious to combine the teachings of Patarin, Shamir, and Patarin2 because there exists a bound to ensure the minimum level of security and it does not have to be a specific number.

6. Claims 12-13, and 29-30 are rejected under 35 U.S.C. 103(a) as being obvious over Patarin in view of Shamir, and further in view of Patarin 'Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two Families of Asymmetric Algorithms' (hereinafter Patarin3).

As per claim 12 and 29, the combination of Patarin-Shamir discloses a method according to claim 4. Patarin does not explicitly disclose said set S2 comprises an expression including k functions that are derived from a univariate polynomial. However, Patarin3 discloses that limitation (Patarin3: page 34: preliminaries). It would have been obvious to one having ordinary skill in the art to combine the teachings of Patarin, Shamir, and Patarin3 because the univariate polynomial is isomorphic to a finite field.

As per claim 13 and 30, the combination of Patarin-Shamir-Patarin3 discloses a method according to claim 12. Patarin3 further disclose univariate polynomial includes a univariate

polynomial of degree n. Same rationale applies here as above in rejecting claim 12. Patarin3 does not explicitly disclose the degree is less than or equal to 100,000. However, Patarin further disclose that limitation (Patarin: column 6 lines 17-35: let $d<=9000$).

7. Claims 37-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin in view of Shamir and further in view of Applicant's Admitted Prior Art (hereinafter AAPA) and further in view of Shamir2.

As per claim 37 and 40, the combination of Patarin-Shamir discloses the method according to claim 1. Patarin-Shamir further discloses coefficients of components involving multiplication of two or more of the n"oil" variables $a_1,\ldots,a_n$ in the k polynomial functions $P'_1(a_1,\ldots,a_{n+v}, y_1,\ldots,y_k)$, ..., $P'_k(a_1,\ldots,a_{n+v}, y_1,\ldots,y_k)$ are zero (Patarin: column 3 line 44-60). Patarin-Shamir does not explicitly disclose said subset S2' being characterized in that all coefficients of components involving orders higher than 1 of any of the n "oil" variables $a_1,\ldots,a_n$ and the number. However, AAPA discloses that limitation (AAPA: page 2-3: the (S) equations are n equations of degree one in the a_i variables when the a'_i variables are fixed). Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Patarin, Shamir, and AAPA because different orders of variables makes it not as clearly distinguishable from the quadratic terms in the published forms thus makes it harder to attack. The combination of Patarin-Shamir-AAPA does not explicitly disclose the number v of "vinegar" variables is greater than the number n of "oil" variables. However, Shamir2 discloses that limitation (Shamir2: page 266: need to modify definition of oil and vinegar domains). Same rationale applies here as above in rejecting claim 6.

As per claim 38 and 41, the combination of Patarin-Shamir-AAPA-Shamir2 discloses the method according to claim 37. Patarin further discloses the set S2 comprises the set S of k polynomial functions of the UOV scheme, and the number v of "vinegar" variables is selected so as to satisfy one of the following conditions (Patarin: column 3 lines 5-22: q is the number of element of K while n is the number of variables which is equal to message or n=m). Patarin does not explicitly disclose the conditions. However, Patarin2 discloses the limitation (a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$ (Patarin2: column 7 lines 45-50: 32 bits and preferably at 64 bits). It would have been obvious to combine the teachings of Patarin, Shamir, and Patarin2 because there exists a bound to ensure the minimum level of security and it does not have to be a specific number.

As per claim 39 and 42, the combination of Patarin-Shamir-AAPA-Shamir2 discloses the method according to claim 37. Patarin further discloses the set S2 comprises a set S of k polynomial functions of a UOV scheme (Patarin: column 3 lines 5-22: q is the number of element of K while n is the number of variables which is equal to message or n=m). Patarin2 further discloses the number v of "vinegar" variables is selected to satisfy the inequalities $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2 where K is a finite field over which the sets S1, S2, and S3 are provided and q is the number of elements of K (Patarin2: column 7 lines 45-50: 32 bits and preferably at 64 bits). Same rationale applies here as above in rejecting claim 38.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Hoffstein et al. U.S. Pat. No. 6076163 discloses secure user identification based on constrained polynomials.

Smith U.S. Pat. No. 5351298 discloses cryptographic communication method and apparatus.

Patarin's 'Asymmetric Cryptography with a Hidden Monomial'.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (703) 305-8654. The examiner can normally be reached on Monday through Friday 8:00am to 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen

Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100
TECHNOLOGY CENTER 2100

Notice of References Cited	Application/Control No. 09/552,115	Applicant(s)/Patent Under Reexamination KIPNIS ET AL.	
	Examiner Shin-Hon Chen	Art Unit 2131	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,111,952	08-2000	Patarin, Jacques	380/45
	B	US-5,790,675	08-1998	Patarin, Jacques	713/180
	C	US-6,076,163	06-2000	Hoffstein et al.	713/168
	D	US-5,351,298	09-1994	Smith, Peter J.	380/30
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Jacques Patarin, 'Asymmetric Cryptography with a Hidden Monomial', Springer-Verlag Heidelberg, Lecture Notes in Computer Science Volume 1109, pages 45-60
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

OIPE AUG 04 2000 PATENT & TRADEMARK OFFICE

PATENT

Sheet 1 of 1

FORM PTO-1449 (Modified) (Rev. 7-80) U.S. Dept. of Commerce Patent and Trademark Office	Atty Docket No. NDS-4600 USA (37597)	Appln. No. 09/552,115
INFORMATION DISCLOSURE CITATION	Applicant(s) AVIAD KIPNIS ET AL.	
(Use several sheets if necessary)	Filing Date April 19, 2000	Group 2766

U.S. PATENT DOCUMENTS

*Examiner Initials		Document Number	Date	Name	Class	Subclass	Filing Date
S.C.	AA	5,263,085	11/16/93	SHAMIR	380	30	11/13/92
S.C.	AB	5,375,170	12/20/94	SHAMIR	380	30	04/19/93

FOREIGN PATENT DOCUMENTS

*Examiner Initials		Document Number	Date	Country	Class	Subclass	Translation YES	NO

OTHER DOCUMENTS

S.C.	AC	PATARIN, J., "HIDDEN FIELD EQUATIONS (HFE) AND ISOMORPHISMS OF POLYNOMIALS (IP): TWO NEW FAMILIES OF ASYMMETRIC ALGORITHMS," EUROCRYPT '96 PROCEEDINGS, MAY 1996, PP. 33-48
S.C.	AD	KIPNIS, A. AND A. SHAMIR, "CRYPTANALYSIS OF THE OIL AND VINEGAR SIGNATURE SCHEME," CRYPTO '98, AUGUST 1998, PP. 257-266
S.C.	AE	KIPNIS, A, ET AL., "UNBALANCED OIL AND VINEGAR SIGNATURE SCHEMES," EUROCRYPT '99, AUGUST '99, PP. 206-222

Examiner	Date Considered
Shin Hon Chen	2/6/04

* Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

RECEIVED AUG -8 2000 TECH CENTER 2700

Asymmetric Cryptography with a Hidden Monomial

and a candidate algorithm for $\simeq$ 64 bits asymmetric signatures

Jacques Patarin

CP8 TRANSAC , 68 route de Versailles - BP 45
78431 Louveciennes Cedex - France
e-mail : J.Patarin@frlv.bull.fr

Abstract

In [1] T. Matsumoto and H. Imai have presented a very efficient "candidate" algorithm, called C^*, for asymmetric cryptography. This algorithm was broken in [2]. Then in [3], I have suggested two algorithms, HFE and IP, to repair C^*. However the secret key computations of HFE and IP are not as efficient as in the original algorithm C^*. Is it possible to repair C^* with the same kind of very easy secret key computations? This question is the subject of this paper. Unfortunately, we will see that for all the "easy" transformations of C^* the answer is no. However one of the new ideas of this paper will enable us to suggest a candidate algorithm for assymetric signatures of length only 64 bits. An extended version of this paper can be obtained from the author.

1 Introduction

In [1] T. Matsumoto and H. Imai have presented a very efficient algorithm C^* for asymmetric cryptography (authentications, signatures or encryptions) with public multivariate quadratic polynomials. This algorithm was based on the idea of "hiding" a monomial equation $b = f(a) = a^{1+2^\theta}$ by two affine permutations s and t. In [2], I have shown that this original algorithm was insecure. Then in [3], I have suggested two new algorithms HFE and IP in order to repair C^*. HFE use more complex hidden functions f (functions f with more than one monomial and sometimes also more than one variable a) but the computation of f^{-1} with the secret key is (of course still feasable but is) more difficult than in C^*. IP is a very different algorithm. It looks like the famous Graph Isomorphisms algorithm.

Is is possible to repair C^* and keeping the same kind of easy secret key computations? For example with multivariate polynomials of total degree 3 or 4 in the public form (instead of two) if necessary? This question is the subject of this paper.

First we will describe two new asymmetric "candidate" algorithms: Dragon and MIIP-3. These algorithms are very efficient. Then we will see that some easier algorithms are insecure. Then we will extend our attacks to see that Dragon with one hidden monomial and MIIP-3 are also insecure.

So it seems that there is not an easy way to "hide" a monomial in order to avoid polynomial attacks ... Nevertheless at the end of this paper, we will show that the idea of "Dragon" Algorithms (however with more than one monomial) gives us a candidate algorithm for extremely short asymmetric signatures. Moreover another family of algorithms (not described here) is still under investigation.

PART 1: Description of the hidden monomial schemes

2 "Dragon": a new family of algorithms for asymmetric cryptography

The public polynomials of the "Dragon" family

The first family of algorithms that we will describe is called "Dragon". Before going into details, let us start by showing the differences between the public polynomials of a scheme like Matsumoto-Imai C^* scheme of [1] and the Dragon schemes.

- In Matsumoto-Imai C^* scheme (or in my HFE scheme of [3]), the public equations are n multivariate polynomials $P_1, \ldots, P_n$ over a finite field K, (n integer), and these polynomials give $y_1, \ldots, y_n$ as functions of $x_1, \ldots, x_n$ like this:

$$\begin{cases} y_1 &= P_1(x_1, \ldots, x_n) \\ y_2 &= P_2(x_1, \ldots, x_n) \\ &\vdots \\ y_n &= P_n(x_1, \ldots, x_n) \end{cases}$$

  where in encryption $(x_1, \ldots, x_n)$ is the cleartext and $(y_1, \ldots, y_n)$ the ciphertext (in signature $(x_1, \ldots, x_n)$ is the signature and $(y_1, \ldots, y_n)$ the message to sign or a public transformation of the message to sign). Moreover in C^* Algorithm the polynomials $P_1, \ldots, P_n$ have total degree 2.

- In the Dragon algorithms that we will describe the public equations are λ multivariate polynomials over a field K (or a ring) like this:

$$\begin{cases} P_1(x_1, \ldots, x_n, y_1, \ldots, y_m) &= 0 \\ P_2(x_1, \ldots, x_n, y_1, \ldots, y_m) &= 0 \\ &\vdots \\ P_\lambda(x_1, \ldots, x_n, y_1, \ldots, y_m) &= 0 \end{cases}$$

  where $P_1, P_2, \ldots, P_\lambda$ are polynomials of $K^n \times K^m \to K$ of small total degree (for example 2, 3 or 4).

As before in encryption $(x_1, \dots, x_n)$ is the cleartext and $(y_1, \dots, y_m)$ the ciphertext (in signature $(x_1, \dots, x_n)$ is the signature and $(y_1, \dots, y_m)$ the message to sign or a public transformation of the message to sign).

So the big difference in the public equations between the Dragon algorithms and Matsumoto-Imai algorithms is that we have "mixed" the variables x_i and y_i.

First example of Dragon in encryption

Here $\lambda = m = n$ and K is a small finite field. Let $q = |K|$ be the number of elements of K. For example $K = F_2 = GF(2)$ the finite field with two elements.

$(x_1, \dots, x_n) \in K^n$ is the cleartext. $(y_1, \dots, y_n) \in K^n$ is the ciphertext. If we have the secrets then we can obtain $(y_1, \dots, y_n)$ from $(x_1, \dots, x_n)$ like this (we will see below another way to compute $(y_1, \dots, y_n)$ from $(x_1, \dots, x_n)$ without any secrets):

1. $x = (x_1, \dots, x_n)$ is first transformed with an affine secret permutation s, so we obtain $s(x) = a = (a_1, \dots, a_n)$.
2. Then a is transformed in b such that

   $$a^{q^\theta + q^\varphi} \cdot M(b) = a^{q^\zeta + q^\xi} \cdot N(b) \qquad (1)$$

   where $\theta, \varphi, \zeta, \xi$ are secret or public integers such that $h = q^\theta + q^\varphi - q^\zeta - q^\xi$ is coprime with $q^n - 1$, $q = |K|$, where the exponentiations are done in a representation of the field $\mathbb{F}_{q^n}$, and where M and N are two affine functions(we will comment the choice of M and N below).

   How do we compute b from a? (We will now give a general way to compute b from a but we will see below that there are sometimes some easier ways). If we write the equation (1) in the components $(a_1, \dots, a_n)$ and $(b_1, \dots, b_n)$ of a and b (i.e. in a basis of F_{q^n}), we will obtain n equations like this:

   $$\sum \gamma_{ijk} a_i a_j b_k + \sum \mu_{ij} a_i a_j = 0 \qquad (2)$$

   where γ_{ij} and μ_{ij} are some coefficients of K.

   The reason for this is that $x \mapsto x^{q^\theta}$ and $x \mapsto x^{q^\varphi}$ are linear functions of F_{q^n}, so $x \mapsto x^{q^\theta + q^\varphi}$ in a basis and $x \mapsto x^{q^\zeta + q^\xi}$ are given by quadratic polynomials.

   Now when $(a_1, \dots, a_n)$ is given the n equations (2) give n equations of degree 1 in the values b_i. So by Gaussian reduction it is then easy (on a computer) to find all the solutions of these equations. We will assume that at least one solution b is found such that $M(b) \neq 0$ or $N(b) \neq 0$. (we will comment this point at the end of this paragraph). If more than one such b is found, we randomly chose one of the solutions for b.
3. Finally $b = (b_1, \dots, b_n)$ is transformed with another affine secret permutation t, so we obtain $t(b) = y = (y_1, \dots, y_n)$.

Remark All these operations are invertibles, so it is possible to compute $(x_1, \dots, x_n)$ from $(y_1, \dots, y_n)$ if the secrets $s, t, \theta, \varphi, \zeta, \xi$ and the representation of the field F_{q^n} are known. For example if $M(b) \neq 0$ then a will be found from b by:

$a = (N(b)/M(b))^{h'}$ where h' is the inverse of $h = q^\theta + q^\varphi - q^\zeta - q^\xi$ modulo $q^n - 1$.

Public computation of $(y_1, \dots, y_n)$ from $(x_1, \dots, x_n)$

The n equations (2) will be transformed in a system of n equations like this:

$$\sum \alpha_{ijk} x_i x_j y_k + \sum \beta_{ij} x_i x_j + \sum \nu_{ij} x_i y_i + \sum \varepsilon_i x_i + \sum \zeta_i y_i + \delta_0 = 0 \tag{3}$$

i.e. n equations $P_i(x_1, \dots, x_n, y_1, \dots, y_n) = 0$, $i = 1, \dots, n$, where P_i is a polynomial of $K^{2n} \to K$, of total degree three. These n equations (3) will be public. They are the public key.

The computation of the n equations (3) from the n equations (2) is done in two steps: first we replace the b_i by their affine expression in y_j and the a_i by their affine expression in x_i (Step 1). Then a linear and bijective transformation u is done on these equations (Step 2).

Note 1. This Step 2 transformation u is secret, or is done in a way to have equations (3) with a conventional presentation (for example the equation number k, $(1 \leq k \leq n)$ will have a term in $x_1 x_2 y_k$ and no terms in $x_1 x_2 y_j$, $j \neq k$: this gives a conventional presentation obtained by Gaussian reductions).

Note 2. We will see in paragraph 4 that the public key length can be moderate despite the fact that the public polynomials are of total degree three. With these public equations (3) anybody will be able to encrypt a message, i.e. to compute $(y_1, \dots, y_n)$ from $(x_1, \dots, x_n)$ without any secret (this is always feasable if there is a value b such that (1) is satisfied).

The reason for this is that when $(x_1, \dots, x_n)$ are given, the n equations (3) give n equations of degree 1 in the values y_i. So by Gaussian reduction it is then easy to find all the solutions of these equations.

Remark. What is unusual with this Dragon Algorithms is that although anybody can compute $(y_1, \dots, y_n)$ from $(x_1, \dots, x_n)$ nobody can express the x_i variables as an effective polynomial in the y_j variables (this polynomial exist but is too large to be explicit if the parameters are well chosen). What is also unusual is the fact that these "Dragon Algorithms" use in a the way the cryptanalysis algorithms of [2] (i.e. with Gaussian reduction) in order to design a new cryptosystems.

The first example of Dragon in signature

It is easy to use this little Dragon Algorithms for asymmetric signatures. For example if $(y_1, \dots, y_n)$ is the message to sign (or a public transformation of the message to sign), then $(x_1, \dots, x_n)$ will be the signature. (The value x corresponding to $a = 0$ may be public in order to avoid this value to be a valid signature of any message).

About the choice of M and N

There are different ways to choose M and N.

Example 1 *In this example, M and N are two secret random affine functions. In signature this Dragon Algorithm is very efficient, but in encryption we may have no solution in b for equation (1).*

However, the probability is high to find a solution b (if q is not too small). (See the extended version for more details). Moreover in the design of the scheme we can decide that a few bytes of the message x have no information, and in the case we find no y for a specific x, we can change these bytes and try again.

Example 2 *In this example $M(b) = b$ and $N(b) = \mu b^{q^\alpha} + \nu b$ where α is an integer such that $q^\alpha - 1$ is coprime with $q^n - 1$ and where μ and ν are two elements of F_{q^n} with $\mu \neq 0$ (but $\nu = 0$ is possible). So the equation (1) is:*

$$a^{q^\theta + q^\varphi} \cdot b = a^{q^\zeta + q^\xi} \cdot (\mu b^{q^\alpha} + \nu b). \tag{4}$$

Now for each $a = 0$ there is exactly only one $b \neq 0$ such that (4) is satisfied.

So this example 2 is an example of candidate trapdoor one way permutation! Moreover here the computation of b from a can be done by square and multiplicity (instead of Gaussian reductions).

Example 3 *In this example $M(b) = b$ and $N(b) = \alpha b + 1$, where α is a secret element of F_{q^n}, $\alpha \neq 0$. So the equation (2) gives*

$$b = 1/(a^{q^\theta + q^\varphi - q^\zeta - q^\xi} - \alpha).$$

So here again we have a candidate trapdoor one way permutation!

3 The algorithm MIIP-3

We will now see a second family of algorithms.

Description of the algorithm

As usual, let K be a finite field. Let L_n be an extension of degree n of K. Let x and y be two elements of L_n. In a basis x is represented by $(x_1, x_2, \dots, x_n)$ and y by $(y_1, \dots, y_n)$ where $\forall i,\ 1 \leq i \leq n$, x_i and y_i are elements of K. Let s and t be two secret affine functions of $K^n \to K^n$. The transformation from x to y can be obtained by these steps (if the secrets are known):

Step 1 Compute $a = s(x)$.

Step 2 Compute (in L_n): $b = a^{1+q^\theta+q^\varphi}$, where $q = |K|$ and θ and φ are two integers, $1 \leq \theta \leq \varphi$, such that $h = 1 + q^\theta + q^\varphi$ is coprime with $q^n - 1$.

Step 3 Finally compute $y = t(b)$.

In a basis each component y_i of y can be written as a polynomial P_i of total degree three in the x_j values, $1 \leq j \leq n$.

These n polynomials P_i, $1 \leq i \leq n$, are made public. So, from these public polynomials, anybody can compute y from x (in encryption y is the encryption of x, and in signature x is the signature of y). Now if the secrets are known it is also easy to compute x from y: each step is easily invertible. But it "seems" that if the secrets are *not* known then x can not be computed for y (we will study this point in paragraph 9).

We call this algorithm MIIP-3: Matsumoto-Imai with Improved Parameters of degree 3. Compared with the original Matsumoto-Imai C^* Algorithm [1] we have made three important changes:

1. There is only **one** branch (i.e. after Step 1, the value a is **not** split in several branches as in [1]). The reason for this will be given in paragraph 5.
2. The transformation $b = f(a)$ gives polynomials of degree **three** (and not two as in [1]). The reason for this is that the cryptanalysis of transformations $b = a^{1+q^\theta}$ was given in [2].
3. The field K is not necessary of characteristic 2. (In [1] the field K was of characteristic 2 in order to find some θ such that $1 + q^\theta$ be coprime with $q^n - 1$. If q is odd this is not possible).

Remark It is very easy to find some bad values for θ and φ. For example if $q = 2$, $\theta = 1$, and $\varphi = 2$, then

$$b = a^7, \text{ so } b \cdot a = a^8 \tag{5}$$

and from this equation (5) it is easy to see that the scheme can be attacked exactly as the original C^* scheme in [2]. However for almost all the choices of θ and φ the attack of [2] does not work against MIIP-3.

Equations (G1), (G2), (G3)

Since $b = a^{1+q^\theta+q^\varphi}$, these three general equations $(G1)$, $(G2)$, $(G3)$ are always satisfied:

$(G1)$ $$a^{1+q^\varphi} \cdot b^{q^\theta} = b \cdot a^{q^\theta(q^\theta+q^\varphi)}$$

$(G2)$ $$a^{1+q^\theta} \cdot b^{q^\varphi} = b \cdot a^{q^\varphi(q^\varphi+q^\theta)}$$

$(G3)$. $$b^{q^\varphi} \cdot a^{q^\theta+q^{2\theta}} = b^{q^\theta} \cdot a^{q^\varphi+q^{2\varphi}}$$

Note. In a basis (G1), (G2), (G3) give $3n$ equations. Generally these $3n$ equations are "formally" independent, i.e. they generate a vector space of dimension $3n$. However if we give some explicit values for b, $b \neq 0$, then we will now prove that (G1), (G2), (G3) will give only 2n independent equations.

Proof Let $A = a^{1+q^\theta}$, $B = a^{1+q^\varphi}$ and $C = a^{q^\theta+q^\varphi}$. Then :

$$(G1) \qquad B \cdot b^{q^\theta} = b \cdot C^{q^\theta}$$

$$(G2) \qquad A \cdot b^{q^\varphi} = b \cdot C^{q^\varphi}$$

$$(G3) \qquad A^{q^\theta} \cdot b^{q^\varphi} = b^{q^\theta} \cdot B^{q^\varphi}$$

and let us assume that b is known, and that A, B and C are unknown. Then from $(G1)$, $(G2)$ and $(G3)$ will we be able to find A, B, and C? No, because $(G3)$ is just a consequence of $(G1)$ and $(G2)$: from $(G1)$ we have $A = b^{1-q^\theta} \cdot C^{q^\theta}$, and from $(G2)$ we have $A = b^{1-q^\varphi} \cdot C^{q^\varphi}$. So $A^{q^\theta} \cdot b^{q^\varphi} = b^{q^\theta - q^{\theta+\varphi} + q^\varphi} \cdot C^{q^{\theta+\varphi}} = b^{q^\theta} \cdot B^{q^\theta \varphi}$. So from $(G1)$, $(G2)$, $(G3)$ we will have only $2n$ independent equations in the $3n$ components (of degree 2 in the x_i) of A, B, and C. (Moreover this proves that if $b \neq 0$, we will always have exactly $2n$ independant equations in the ($\simeq 3n$) components of A, B and C).

4 Implementations and public key lengths

The algorithms Dragon and MIIP-3 that we have seen are very efficient. These algorithms are fast and can easilly be implemented in smartcards with low power (without arithmetic coprocessor). Moreover we will see now that the public key length can be very moderate for two reasons:

1. We can have a value n which is not too large (for example $n = 32$) if we have a value q which is not too small.
2. Moreover, the public key can be written with polynomials of total degree two (instead of three) as we will see now! (Unfortunately this idea will help us to attack the schemes as we will see in Part 2).

Dragon

In the Dragon algorithms of paragraph 2, the hidden equation is:

$$a^{q^\theta+q^\varphi} \cdot M(b) = a^{q^\zeta+q^\xi} \cdot N(b). \qquad (6)$$

For simplicity of the equations let us assume that s and t are linear (if s and t are affine the same results will also hold). The public key, computed from this equation (6) is a set of n equations like this:

$$\sum_i \gamma_{ijkl} x_j x_k y_l = 0. \qquad i = 1, \ldots, n.$$

Let $P_{il} = \sum_{j,k} \gamma_{ijkl} x_j x_k$. We have $O(n^2)$ such values P_{ij}. But how many independant such P_{il} will we have? In fact at most $2n$ because in the hidden equations (6) we have n components from $a^{q^\theta+q^\varphi}$ and n components from $a^{q^\zeta+q^\xi}$. So all the P_{il} can be written as a linear expression in only λ variables, $\lambda \leq 2n$, that we will call $p_1, \dots, p_\lambda$. So we see that the public key can always be written (without changing the security since this new public key can be computed from the original in polynomial complexity) as two sets of equations.:

$$p_i = \sum_{j,k} \nu_{ijk} x_j x_k \qquad (i = 1 \text{ to } \lambda, \quad \lambda \leq 2n)$$

$$\sum_{j=1}^{\lambda} \sum_{k=1}^{n} \xi_{ijk} p_j y_k = 0 \qquad (i = 1 \text{ to } n).$$

In these new public equations we will have only $0(n^3)$ terms instead of $0(n^4)$ terms in the original presentation.

Note. If $a^{q^\theta+q^\varphi}$ is not a linear transformation of $a^{q^\zeta+q^\xi}$ then $\lambda = 2n$ with a very high probability. It is not clear if λ can be $\neq n$, $\simeq 2n$ and $< 2n$ and what cryptanalysis can be done if this occur.

MIIP-3

Similarly, from the public key of a MIIP-3 algorithm it is always feasable to compute all the equations $\sum \gamma_{ijk} x_i x_j y_k + \cdots = 0$ that are always true when x is the encryption of y, and to see that the terms in the y_k variables are generated by only about $0(n)$ polynomials of degree two. The fact that we always have such polynomials come from the (G1), (G2), (G3) equations. If we denote by $P_1, \dots, P_\lambda$ these polynomials ($\lambda = 0(n)$ and $\lambda = 3n$ very often), then instead of the public key we can write (without changing the security) about μ equations like this, $\mu \simeq 3n$:

$$\sum_{k=1}^{n} \sum_{j=1}^{\lambda} \xi_{ijk} p_j y_k + \sum \mu_{ij} p_j + \sum \nu_{ij} y_j + \delta_i = 0, \quad 1 \leq i \leq \mu.$$

(Most of these equations come from (G1), (G2), (G3). However sometimes we will have $\mu \simeq 4n$ or $\mu \simeq 5n$ when we will have more equations than (G1), (G2), (G3). But μ is always such that $\mu \simeq kn$, with k small and $k \geq 3$).

These equations plus the definitions of $p_1, \dots, p_\lambda$ are the new public key and we have about $0(n^3)$ terms in the new public key instead of $0(n^4)$ terms in the original public key.

Note. The designer of the scheme can choose to make public only a part of these equations, for example these coming from (G1). This may make the attack

easier (as we will see in Part 2) since he has isolate (G1) from (G2) and (G3). However since anybody can compute the set of all the equations as above it does not change de security, from the polynomial complexity point of view, to present this set of $0(n^3)$ equation as the new public key.

PART 2: Cryptanalysis results

5 Cryptanalysis of extended Matsumoto-Imai Algorithms with small branches

In the description of the original Matsumoto-Imai C^* algorithm given in [1], after the first affine transformation s, the inputs are divided in d branches. We have not made such a separation in our description of Dragon and MIIP-3, because we have found three very general attacks against small branches. We describe these three attacks in the extended version of this paper. These three attacks are very instructive and they are based on three completely different ideas. The first one uses some algebraic equations, and the second one is based on differential cryptanalysis.

6 Cryptanalysis of two compositions of C^* algorithms

A very natural idea, in order to keep a bijective cryptosystem with easy secret computations is to do the composition of two C^* Matsumoto-Imai Algorithms. Of course one problem is that the public polynomials will be of total degree four (instead of two) but if n is not too big, so if $K = \mathbb{F}_q$ is not so small ($q = 2^\mu$, with $\mu \neq 1$), then the length of the public key may still be acceptable. However we show in the extended version of this paper a bigger problem: such a scheme remains insure.

We will just give here the idea of the attack. It is to compute all the equation of this form:

$$\sum_i \sum_j \sum_k \mu_{ijk} y_i x_j x_k + \sum_i \sum_j \nu_{ij} x_i x_j + \sum_i \sum_j \xi_{ij} y_i x_j + \sum_i w_i x_i + \sum_i \theta_i y_i + \pi_0 = 0.$$

Then we will introduce some "transition" variables p_i such that these equationscan be written like this:

$$\sum_i \sum_j \gamma'_{ij} p_i y_j + \sum_i \alpha'_i p_i + \sum_i \beta'_i y_i + \delta'_0 = 0$$

when the y_i variables are given, then from these equations we will be able to find the p_j variables (by Gaussian reduction). Then we will find x from the p_j variables as in the attack of [2].

7 Cryptanalysis of the little Dragon Algorithm

Introduction

In this paragraph we will study the cryptanalysis of the "little Dragon" algorithm. What we call "little Dragon algorithm" is the algorithm where instead of equation (1) (of paragraph 2.2) the hidden equation is:

$$a \cdot b = a^{q^\theta + q^\varphi}, \tag{7}$$

where θ and φ are secret integers such that $h = q^\theta + q^\varphi - 1$ is coprime with $q^n - 1$. Since there are not a lot of possible values for θ and φ we can also assume that θ and φ are public.

This algorithm looks very interesting because the public equations computed from (7) are only of total degree two. However this algorithm is insecure, as we will see now.

Cryptanalysis of the scheme

We will assume here that the secret functions s and t are linear (not only affine). This probably does not change a lot of things (moreover there the value $a = 0$ can very easily be detected so we can clearly assume that s is linear). So the public equations comming from (7) is a set of n equations like this:

$$\sum_{j,k} \gamma_{ijk} x_j y_k + \sum_{j,k} \mu_{ijk} x_j x_k = 0, \qquad 1 \le i \le n. \tag{8}$$

Let $\delta_i = \sum \gamma_{ijk} x_j y_k$, $1 \le i \le n$. The values δ_i are public and they represent the "hidden" components of $a \cdot b$. We denote by $\delta = (\delta_1, \ldots, \delta_n)$.

The cryptanalysis is in four steps.

Step 1 We compute the vector space of all the linear transformations C and D such that:

$$\forall i, \quad 1 \le i \le n, \quad (C(\delta))_i = \sum_{j,k} \gamma_{ijk} x_j (D(y))_k. \tag{9}$$

This set will by found by Gaussian reductions on the values of the C and D matrices.

We are sure to find a vector space of solutions of dimension at least n since we have :

$$\forall \lambda \in F_{q^n}, \quad \lambda(a \cdot b) = a \cdot (\lambda b).$$

So each transformation $b \mapsto \lambda b$ gives a couple (C, D) of matrices solution.

Moreover I did a small simulation and in this simulation I found a dimension exactly n for the set of solutions. For simplicity, let us assume that we have exactly such a dimension n of solutions.

Since the set of solutions found for D depends on n free variables, we can call these variables $\Lambda_1, \Lambda_2, \ldots, \Lambda_n$, and we can denote $\Lambda = (\Lambda_1, \ldots, \Lambda_n)$, and

D_Λ the solution with the parameter Λ. We will also denote by $D_\Lambda(y)$ the vector of components $(D_\Lambda(y_1), \ldots, D_\Lambda(y_n))$.

Step 2 We compute the vector space of all the linear transformations E such that :

$$D_{E(\Lambda)}(y) = D_{E(y)}(\Lambda).$$

Here again we expect to find a vector space of dimension n (and indeed this is what I found in my small simulation). Let E_0 be such a solution and let $*$ be the operation such that by definition:

$$\Lambda * y = y * \Lambda = D_{E_0(\Lambda)}(y).$$

Remark If we denote by t the secret affine transformation from b to y, then there will be an element $\mu \in F_{q^n}$, $\mu \neq 0$, such that:

$$\Lambda * y = t(\mu \cdot t^{-1}(\Lambda) \cdot t^{-1}(y)).$$

So t and μ are not known, but such an operation $*$ has been found.

Step 3 Let $h = 1 + q^\theta + q^\varphi$, so $b = a^h$, and let h' be the inverse of h mod $2^n - 1$, so $a = b^{h'}$. We can assume that h' is public because there are not a lot of possible values for θ and φ (so the cryptanalyst can try one by one all the solutions).

Let f be the function : $f(y) = y^{h'}$, where $y^{h'}$ denotes $y * y \cdots * y$, h' times. (This function f is computed by square and multiply from the operation $*$). Then we have: $f(y) = t(\mu^{h'-1} b^{h'}) = t(\mu^{h'-1} a)$ (where b denotes $t^{-1}(y)$ as usual). So $f(y) = W(x)$, where x is the cleartext and W an affine function! So from f it is easy to find W by Gaussian reductions on a few cleartext/ciphertext couples.

Step 4 *Now that f and W are found it is easy to decrypt any message since:* $x = W^{-1}(f(y))$.

8 Cryptanalysis of the Dragons of paragraph 2

Now we will give an algorithm for the cryptanalysis of the Dragon scheme given in paragraph 2.

For simplicity we will assume that M (or N) is bijective and that s and t are linear. (This probably does not change much). So we can assume that the hidden equation is:

$$a^{q^\theta + q^\varphi} \cdot b = a^{q^\zeta + q^\xi} \cdot N(b).$$

Since s and t are linear we know from paragraph 4 that the public key can be given as a set of about $2n$ equations like this: $p_i = \sum_{j=1}^{n} \sum_{k=1}^{n} \nu_{ijk} x_j x_k$, $1 \leq i \leq 2n$,

plus a set of n equations like this: $\sum_{j=1}^{2n}\sum_{k=1}^{n}\xi_{ijk}p_j y_k$, $1 \le i \le n$. (From the public key it is always feasable to find these two sets of equations).

Let $\delta_i = \sum_{j=1}^{2n}\sum_{k=1}^{n}\xi_{ijk}p_j y_k$. The values δ_i, $1 \le i \le n$ are public. We denote by $\delta = (\delta_1, \dots, \delta_n)$, and by $p = (p_1, \dots, p_{2n})$. The cryptanalysis is in four steps.

Step 1 We compute (by Gaussian reductions) the vector space of all the linear transformations C and D such that:

$$\forall i, \quad 1 \le i \le n, \quad (C(\delta))_i = \sum_{j=k}^{2n}\sum_{k=1}^{n}\xi_{ijk}(D(p))_j y_k.$$

C is a $n \times n$ matrix and D is a $2n \times 2n$ matrix.

We are sure to find a vector space of solutions of dimension at least n since we have :

$$\forall \lambda \in F_{q^n}, \quad \lambda(a^{q^\theta+q^\varphi} \cdot b - a^{q^\zeta+q^\epsilon} \cdot N(b)) = (\lambda a^{q^\theta+q^\varphi}) \cdot b - (\lambda a^{q^\zeta+q^\epsilon}) \cdot N(b).$$

So each transformation $(a^{q^\theta+q^\varphi}, a^{q^\zeta+q^\epsilon}) \mapsto (\lambda a^{q^\theta+q^\varphi}, \lambda a^{q^\zeta+q^\epsilon})$ gives a couple (C, D) of matrices solution.

Step 2 Let D_0 be such a solution, with $D_0 \neq 0$. Then we will find an invertible matrix S such that $D_0 = S^{-1}D_0'S$ where

$$D_0' = \begin{pmatrix} D_1 & \vdots & 0 \\ \dots & \vdots & \dots \\ 0 & \vdots & D_2 \end{pmatrix}$$

where D_1 and D_2 are two $n \times n$ matrices. (This is feasable from the matrices reduction theory, however I did no simulation. See for example [4]). D_1 will come from $a^{q^\theta+q^\varphi} \mapsto \lambda a^{q^\theta+q^\varphi}$ and D_2 will come from $a^{q^\zeta+q^\epsilon} \mapsto \lambda a^{q^\zeta+q^\epsilon}$.

Step 3 The matrix S gives a change of variables on the p_i variables: let $p_1', \dots, p_n'$ be the terms changed by D_1 and $q_1', \dots, q_n'$ be the terms changed by D_2. Then the n equations δ_i can be rewritten in n equations like this:

$$\sum_{j=1}^{n}\sum_{k=1}^{n}\mu_{ijk}y_j p_k' = \sum_{j=1}^{n}\sum_{k=1}^{n}\gamma_{ijk}y_j q_k', \qquad 1 \le i \le n.$$

Step 4 Let $\delta_1', \dots, \delta_n'$ be the terms of the left side of this equation:

$$\delta_i' = \sum_{j=1}^{n}\sum_{k=1}^{n}\mu_{ijk}y_j p_k'. \qquad 1 \le i \le n.$$

These terms come from $a^{q^\theta+q^\varphi}\cdot b$. From these terms we will find an operation $\Lambda * y$ exactly as we did for the little Dragon algorithm. So if $a = b^{h'}$ (as in paragraph 2 example 2 with $\nu = 0$ or as in the (G1) equation of MIIP-3) then we will just compute $y^{h'}$ with this $*$ operation. What about more general cases, i.e. when the transformation from b to a is more complex than $b = a^{h'}$? Due to the lack of space please see the extended version of this paper. (The idea is to find the analogy of $b \mapsto (N(b)/b)^{h'}$ in y with the $*$ operation as the basic operation on y).

9 Cryptanalysis of MIIP-3

Now we will give an algorithm for the cryptanalysis of the MIIP-3 algorithm. For simplicity we will assume that s and t are linear (this probably does not change a lot of things). Since s and t are linear we know from paragraph 4 that the public key can be given as a set of about $3n$ equations like this (sometimes more): $p_i = \sum_{j=1}^{n}\sum_{k=1}^{n} \nu_{ijk}x_jx_k$, $1 \le i \le 3n$, plus a set of about $3n$ equations like this: $\sum_{j=1}^{3n}\sum_{k=1}^{n} \xi_{ijk}p_jy_k = 0$, $1 \le i \le 3n$. These equations come from

$$(G1): B\cdot b^{q^\theta} = b\cdot C^{q^\varphi}, (G2): A\cdot b^{q^\varphi} = b\cdot C^{q^\varphi}, (G3): A^{q^\theta}\cdot b^{q^\varphi} = b^{q^\theta}\cdot B^{q^\varphi}$$

where $A = a^{1+q^\theta}$, $B = a^{1+q^\varphi}$, and $C = a^{q^\theta+q^\varphi}$. (Sometimes we have more than these $3n$ equations, but for simplicity we will assume that there are only these $3n$ equations and that they give a vector space of dimension $3n$).

Let $\delta_i = \sum_{j=1}^{3n}\sum_{k=1}^{n} \xi_{ijk}p_jy_k$. The values δ_i, $1 \le i \le 3n$, are public. We denote by $\delta = (\delta_1, \ldots, \delta_{3n})$ and by $p = (p_1, \ldots, p_{3n})$. The cryptanalysis is in three steps.

Step 1 We compute (by Gaussian reductions) the vector space of all the linear transformations D and E such that:

$$\forall i, \quad 1 \le i \le n, \quad (E(\delta))_i = \sum_{j=k}^{3n}\sum_{k=1}^{n} \xi_{ijk}(D(p))_jy_k.$$

E is a $3n \times 3n$ matrix and D is also a $3n \times 3n$ matrix.

We are sure to find a vector space of solutions of dimension at least n since we have : $\forall\lambda \in F_{q^n}$, if B is changed in $\lambda^{q^\theta}B$, C in λC and A in $\lambda^{q^\varphi}A$, then $(G1)$ is changed in $\lambda^{q^\theta}(G1)$, $(G2)$ in $\lambda^{q^\varphi}(G2)$ and $(G3)$ in $\lambda^{q^\theta+q^\varphi}(G3)$.

Step 2 Let E_0 be such a solution for E, with $E_0 \ne 0$. Then we will find an invertible matrix S such that $E_0 = S^{-1}E'_0S$ where

$$E'_0 = \begin{pmatrix} E_1 & \vdots & 0 & \vdots & 0 \\ \cdots & \vdots & \cdots & \vdots & \cdots \\ 0 & \vdots & E_2 & \vdots & 0 \\ \cdots & \vdots & \cdots & \vdots & \cdots \\ 0 & \vdots & 0 & \vdots & E_3 \end{pmatrix}$$

(This is feasable from the matrices reduction theory. See for example [4]).

E_1 comes from $(G1) \rightarrow \lambda^{q^\theta}(G1)$, E_2 comes from $(G2) \rightarrow \lambda^{q^\varphi}(G2)$ and E_3 comes from $(G3) \rightarrow \lambda^{q^\theta+q^\varphi}(G3)$.

Step 3 From S we can isolate the equation $(G1)$ from the other equations, and so attack the scheme as a Dragon scheme as we did in paragraph 8.

Remark. For MIIP-4 (i.e. with the hidden equation $b = a^{1+q^{\theta_1}+q^{\theta_2}+q^{\theta_3}}$) the same kind of polynomial attack exists.

10 Unclear cases

In all the schemes. Is the cryptanalysis more difficult if the transformations s and t are affine (instead of linear)? (Probably not, but I did not check).

For MIIP-3 and C^*. In MIIP-3, with the original public form, or in C^*, what do we do if 2 or 3 of the public polyomials are not given? The scheme will still work in signature, and also in encryption if we had redundancy, but may be more difficult to attack. (However if only one equation is not given with $n = 64$ and $K = F_2$ then from the Birthday paradox we will easilly be able to find this equation).

PART 3: A candidate for 64 bits signatures and conclusion

11 A candidate Dragon algorithm for extremely short signatures

$\forall a \in F_{q^n}$, $\forall b \in (F_q)^{2n}$, let

$$f(a,b) = \sum_{i=1}^{k} \alpha_i a^{q^{\beta_i}+q^{\gamma_i}} N_i(b) + \sum_{i=1}^{k'} \alpha'_i a^{q^{\beta'_i}} N'_i(b) + \delta_0,$$

where for all the indices i we have: α_i, α'_i, $\delta_0 \in F_{q^n}$, β_i, γ_i, β'_i, k and k' are integers, N_i and N'_i are affine functions of $(F_q)^{2n} \rightarrow F_{q^n}$ (as usual affine means

affine over F_q), and where the degree d in the a variable is not too large (for example $d \leq 8000$).

Then let $a = s(x)$ and $b = t(y)$ where s and t are two secret affine permutations. In a basis $f(a, b) = 0$ gives n equations of total degree three (degree two in a_i and one in b_i variables). These n equations will be writen in x_i and y_j variables (Step 1) and then a linear and bijective transformation is done on these equations (Step 2). We obtain like this a set (G) of n equations of total degree three (degree two in x_i and one in y_i variables). (G) is public. f is secret (this function is "hidden" by s and t).

For example $q = 2$, $n = 64$, and in f we have all the monomials $a^{2^{\beta_i}+2^{\gamma_i}}$ and all the monomials $a^{2^{\beta'_i}}$ with $2^{\beta_i} + 2^{\gamma_i} < 8000$ and $2^{\gamma_i} < 8000$, and α_i and α'_i are randomly chosen in F_{q^n}, and N_i and N'_i are also randomly chosen.

Let M be a message to sign. The signature of M is $(x||R)$ where R is any small integer with no pattern 1000 in its expression in base 2 (for example $R = 0$). x is any 64 bits value such that if we denote $y =$ Hash $(R||1000||M)$, then (x, y) satisfies all the n equations of (G). Here Hash is a collision free Hash function with 128 bits outputs (for example Hash $= MD5$), and $||$ is the concatenation function. So anybody can verify a signature (x, R) without any secret. In order to compute the signature we will compute $b = t^{-1}(y)$, then we will solve in a the equation $f(a, b) = 0$ (this is always feasable with a complexity polynomial in d). If there is no solution, we try with another value R (for example $R = 1$ instead of $R = 0$) until we find a solution a. Then $x = s^{-1}(a)$ is computed. On average the length of the signature (R, x) will only be about 64 bits. (Moreover we can also give only x as the signature and all the small values of R will be tried one by one to check the signature). We avoid the "birthday paradox" since we can not publicly compute y from x but just check if x and y match together or not. However the time to compute a signature is long so this scheme is not very efficient. Its interest lies in the fact that it is the first candidate algorithm with 64 bits asymmetric signatures (I do not know any previous candidate). The best attack that I know against this scheme needs more than 2^{50} computations. With 80 bits signature this attack needs more than 2^{64} computations. Moreover after these computations, only one signature is found: to compute another signature the same huge computations are needed.

This algorithm is still a Dragon algorithm (since x and y are mixed) but with a hidden function instead of a hidden monomial.

Note 1 These attacks are based on the idea to do exhaustive search on $n - k$ variables x_i, k small, and to find the k other variables from the public equations. I was no able to see somebody who knows if a better attack is known to solve a randomly set on n quadratic equations over $GF(2)$ when $n \simeq 64$. I will try to have the efficiency of the known algorithms for the conference in August. Maybe $n = 64$ is easy even for random quadratic equations?

Note 2 For any signature scheme with signatures of length 64 bits that can sign messages of arbitrary length, after about 2^{32} signatures two messages signed have the same signature. However here the collision is obtained between two messages

signed by the owner of the secrets, and moreover only after 2^{32} signatures, made by himself. So this may not be a problem.

Note 3 The function f (as in a variation of HFE) can also be more general, as long as in a basis $f(a,b)$ is of small degree in a_i and b_i variables and the computation of a such that $f(a,b) = 0$ is feasable. For example a multivariate resolution algorithm with a few variables (8 equations with 8 variables for example with each variable on 8 bits) will be hidden as an intractable system of 64 equations with 64 variables a_i and 64 variables b_i by s and t.

12 Conclusion

In this paper, we have studied some algorithms based on the idea of a "hidden" monomial. The motivation was that these algorithms are very efficient and that some of these algorithms were candidate trapdoor one way permutations. Unfortunately we have seen that all the easy transformations of C^* can be attacked in polynomial complexity. (Some simulations would be require to test the validity of the attacks). We have also described a candidate algorithm for 64 bits signatures that has so far resisted all attacks. However this algorithm is not very efficient and also has no proof of security. So at present, the two algorithms of [3] seem to remain the best candidates to try to repair the C^* algorithm of [1].

Acknowledgments

I want to thank Isabelle Guerrin-Lassous for doing a lot of simulations, Henri Gilbert for his help in the design of the differential attack of paragraph 5; also Frédéric Charbonier, Tsutomo Matsumoto, Louis Gaubin and Paul Camion for useful comments. Finally I would like to give special thanks to an anonymous referee of Crypto'96 for giving the idea to study the transformation $b \mapsto \lambda b$ on the public equations of the little Dragon algorithm...

References

[1] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption", EUROCRYPT'88, Springer Verlag, pp. 419-453.

[2] J. Patarin, "Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88", CRYPTO'95, Springer Verlag, pp. 248-261.

[3] J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new Families of Asymmetric Algorithms", EUROCRYPT'96, Springer Verlag, pp. 33-48.

[4] F.R. Gantmacher, "The theory of matrices", Chelsea Publishing Company, Volume one, chapter VII.